Teri Takai

California State CIO

OCIO Vendor Forum

February 23, 2009

OCIO
Office of the State
Chief Information Officer

What are we going to talk about today?

- The OCIO year in review
- What’s planned for the future
- Where do private companies fit in?

OCIO – One year later

- Created in 2008
- Aligning IT and business priorities
- Modernizing California's approach to IT

Early, the OCIO stated a number of goals in the 2008 May 15th Report to the Legislature…

Office of the State Chief Information Officer

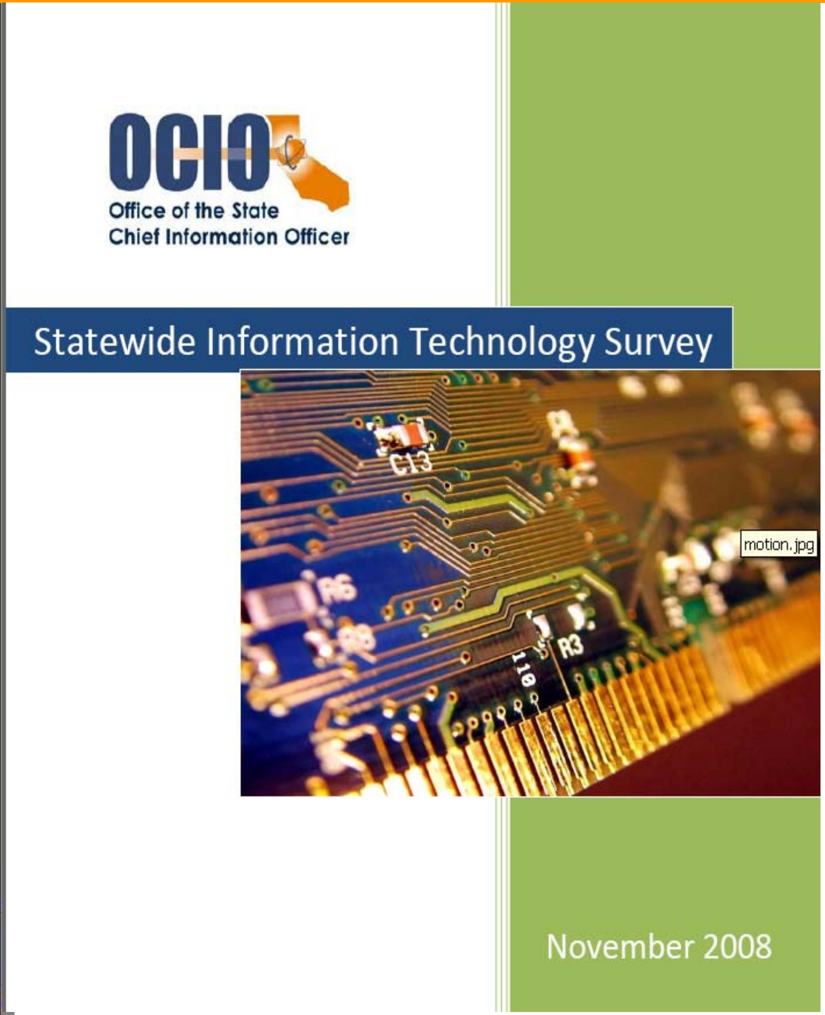
Moving forward – the May 15th Report

- Integrated Business and IT Planning
- Enterprise Architecture
- Project Management
- Comprehensive Data Strategy
- Develop and Retain Key IT Skills

In short, our goal is to bring a modern, enterprise IT program to California. But before we moved forward, we needed to survey our current assets…

OCIO
Office of the State
Chief Information Officer

Statewide Survey



Office of the State Chief Information Officer

Statewide Information Technology Survey

motion.jpg

November 2008

- *$3 billion*
- *130* CIOs
- *10,000 IT staff*
- *409,000 sq. ft. of datacenters*
- 9,494 servers
- 180,000 mailboxes

Office of the State Chief Information Officer

Agencies and Departments submitted 5-year Capital Plans, detailing their planned investments…

5-year IT Capital Plan

First Global view of upcoming projects and business priorities

- Department IT Capital Plan
- Agency IT Capital Plan

The OCIO needed to do more than just compile information; we needed to provide leadership by projecting a future vision of IT in California…

OCIO
Office of the State
Chief Information Officer

California IT Strategic Plan Vol. I

- Put together by AIOs and working groups throughout the state
- Six major strategic concepts

www.itsp.ca.gov

OCIO
Office of the State
Chief Information Officer

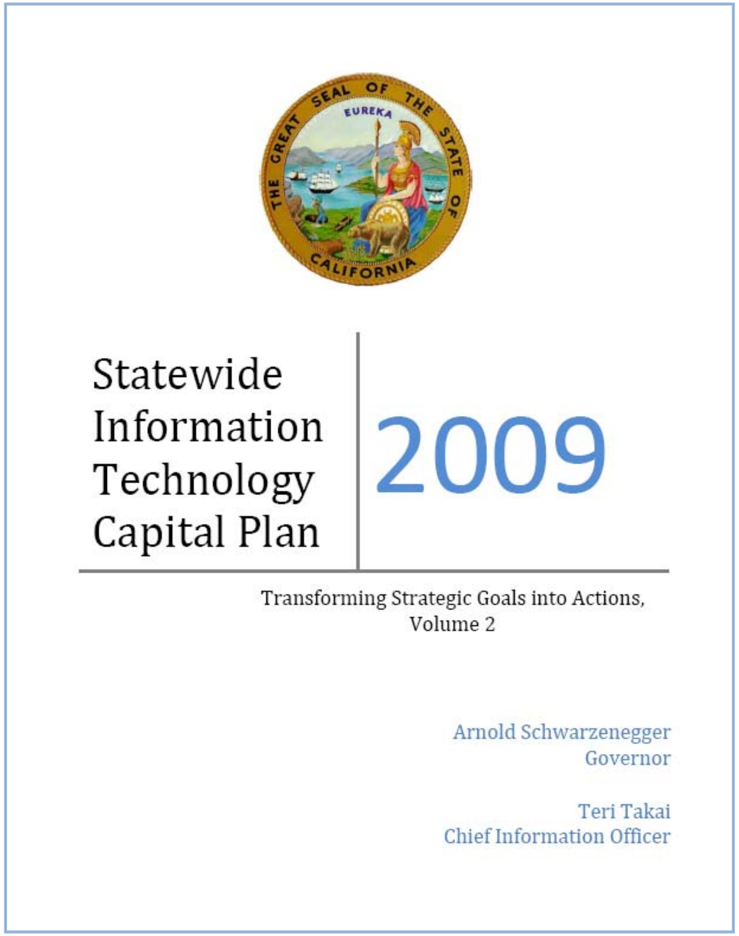
Six strategic concepts

1. IT as reliable as electricity
2. Fulfilling technology’s potential to transform lives
3. Self-Governance in the digital age.
4. Information as an asset
5. Economic and sustainable
6. Facilitating collaboration that breeds better solutions

The Strategic Concepts are aspirational, grounding them in business direction gives them meaning…

OCIO Office of the State Chief Information Officer

Strategic Plan Vol. II – Statewide ITCP



Statewide Information Technology Capital Plan

2009

Transforming Strategic Goals into Actions, Volume 2

Arnold Schwarzenegger
Governor

Teri Takai
Chief Information Officer

- 122 new approved project-concepts
- Each concept is mapped to a strategic goal
- OCIO, Finance will develop these concepts further
- 70 percent of concepts have collaborative opportunities

With a statewide strategic direction and a view of business priorities, the OCIO is ready to turn strategies into action…

OCIO
Office of the State
Chief Information Officer

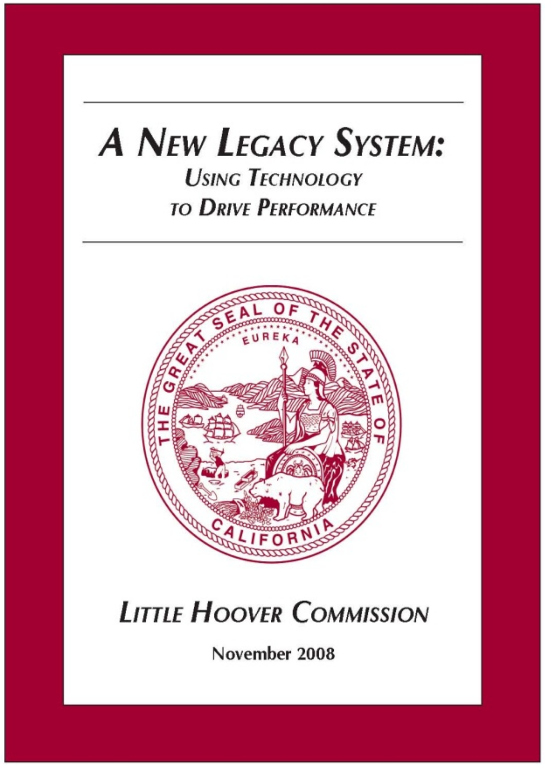
Upcoming: Strategic Plan Vol. III – Strategies in Action

- Legislatively-mandated report
- Tactical component of strategic plan
- Written by IT and Business leaders
- Actionable items included

This vision of IT in California balances statewide standards and business priorities, but are we organized to fulfill this vision…

Governor’s Reorganization Plan

- Based on Little Hoover Commission Recommendations
- LHC hearing on the GRP to be held on February 25th
- Consolidate four organizations into one, under OCIO



A NEW LEGACY SYSTEM:
USING TECHNOLOGY
TO DRIVE PERFORMANCE

LITTLE HOOVER COMMISSION

November 2008

Consolidated organizations

- OCIO
- Department of Technology Services
- OISPP – Information Security functions
- DGS – Telecommunications division

The GRP also clarifies the relationship between state agencies and the OCIO…

Federated Governance Model

"The state CIO must be given the authority to set and execute technology priorities as laid out in the state's IT Strategic Plan. The state CIO must be given the resources to accomplish the task." ~Little Hoover Commission, November 2008

Enterprise Tier (OCIO)

Statewide infrastructure
Shared services
Common applications

Agency Tier

Business direction
Investment authority
Consolidated IT resources

Department Tier

Desktop/LAN support
IT purchases
Program-level applications

What are the first steps to implementing the Federated Governance Model…

OCIO
Office of the State Chief Information Officer

Upcoming: Agency Consolidation Plans

- Implement Federated Governance Model
- Organize IT employees under AIOs, CIOs
- Create robust infrastructure

I'm sure you all want to know, how the GRP is going to affect IT procurement…

OCIO
Office of the State
Chief Information Officer

Procurement in the GRP

The OCIO will assume responsibility for IT procurement policy. I want to set policies that…

Office of the State Chief Information Officer

Changes in Procurement

- Ensure procurements driven by technology standards
- Standardize the process for acquiring technology
- Make requirements that enable more competition
- Make vendors a partner in transforming California

OCIO
Office of the State
Chief Information Officer

Partnership is a two-way street

What we need from you

- Read the strategic plan and understand the state's aspirational direction, its business priorities and our tactical plan
- Be patient, we will get to you
- Participate in future vendor events

OCIO
Office of the State
Chief Information Officer

DGS

Assembly Bill 617 (Torrico) Financial Risk Mitigation

February 23, 2009

Welcome

- Preview consultant findings
- Provide risk assessment framework
- Propose a tool for use by the State to mitigate financial risk for large IT projects
- DGS pilot project
- Update framework and tool

Procurement Reform

Assembly Bill (AB) 617 tasked DGS and DOF to develop and maintain:

- Criteria for the evaluation of State IT acquisition risk
- A risk mitigation framework and a tool to protect the State from financial loss

Consultant’s Findings

- Other states generally do not use performance bonds; nearly all do not use letters of credit
- Federal government does not support performance bonds
- Most states use liquidated damages and withholds
- Limitation of Liability is frequently negotiated by other states and ranges from contract value to as much as 5 times contract value

Financial Risk Mitigation

- Focused on project risks that can be mitigated during the acquisition/contract phase
- Tailors risk factors to each bidder’s proposal
- Applies appropriate financial risk mitigation mechanism(s)
- Provides financial protection to the State
- Reduces risk to the Contractor

Recommendations

- Payment Withhold: Up to 20% for very high risk proposals
- Liquidated Damages: Clearly defined criteria for applying LDs to mitigate risk to the Contractor
- Limitation of Liability: Assessed based on project risk score (1x-2x)
- Deliverables are self contained and hold independent value to the State (not considered progress payments)
- Option for Performance Bond or Letter of Credit (this will be clearly defined in the solicitation)

Risk Mitigation Mechanisms

Total Project Risk Percentage	Withholds	Limitation of Liability	Liquidated Damages	Independent Deliverables	Optional Performance Bond	Optional Letter of Credit
High	X	X	X	X	X	X
Medium	X	X	X	X		
Low	X	X				

Progress Payment Withhold:

- **Low Risk Projects – 10% withhold**
- **Medium Risk Projects – 10% withhold**
- **High Risk Projects – 10-20% withhold (depending on the individual bidder proposal)**

Limitation of Liability:

- **Low Risk Projects - 1X liability**
- **Medium Risk Projects – 1.5X liability**
- **High Risk Projects – 2X liability**

Financial Risk Factors

Consider 25 factors, including but not limited to:

- Project cost (based on the State’s estimate)
- Legislatively mandated/Public health and safety
- Degree of integration
- Proposed system solution (COTS, MOTS, Custom)
- Bidder experience and track record
- Bidder financial stability

Applying the Framework

- Unique risk score for each proposed solution
- Risk scoring factors are published in the solicitation
- Risk is assessed during draft proposals
- Bidders will be informed of the required risk mitigation mechanisms for their proposed solution before confidential discussions

Framework Test Plan

- Pilot project within DGS/PD
- Testing and validation of risk factors
- Accurate data collection of risk mitigation mechanisms used
- Traceability to mitigation of State risk
- Ability to modify framework based on project data collection and traceability findings

Automated Tool

- Automated tool will be available on the DGS/PD web page
- DGS will utilize tool for projects that include progress payments
- Automated tool will be modified and updated as the risk framework is continuously improved

Next Steps

- Financial Risk Mitigation Report is being reviewed and finalized by DGS and DOF
- Review by DGS Legislative Affairs Office
- Review by State and Consumer Services Agency
- Submit to the Joint Legislative Budget Committee and the State Chief Information Office
- Pilot Implementation

Discussion

- Discussion

- Thank you

  Jim Butler, Deputy Director, Procurement Division

DTS Update

P.K. Agarwal
February 23, 2009

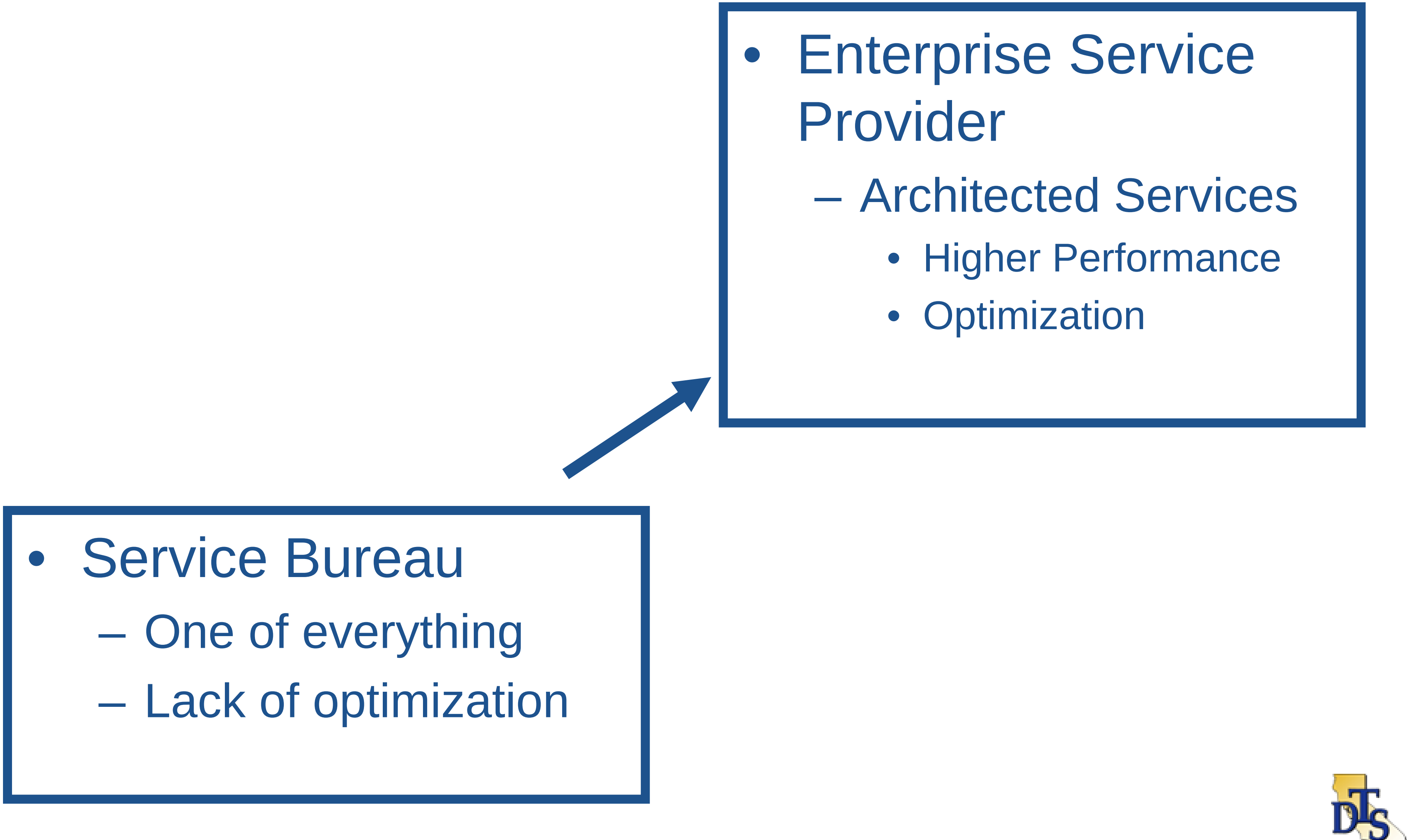
Topics

- Strategic Change at DTS
- Enterprise Projects
  - Cannery Relocation
  - Network Consolidation
  - Statewide eMail
  - eServices

Data Center Challenges

- Virtualization
- Green
- ITIL
- SLA’s
- Cloud Computing
- Managed Services
- Security
- Cost

A Strategic Transition



- Enterprise Service Provider
  - – Architected Services
    - Higher Performance
    - Optimization

- Service Bureau
  - – One of everything
  - – Lack of optimization

DTS Strategic Goals

Customer Satisfaction

Employee Investment

Financial Viability

Process Improvement

Enabling Investments

Technology Leadership

Enterprise Projects

Cannery Relocation

Why?

- Aging Physical Infrastructure
- Improve Security of State’s Data by Geographic Separation of Sites
- Position for Improved Disaster Recovery

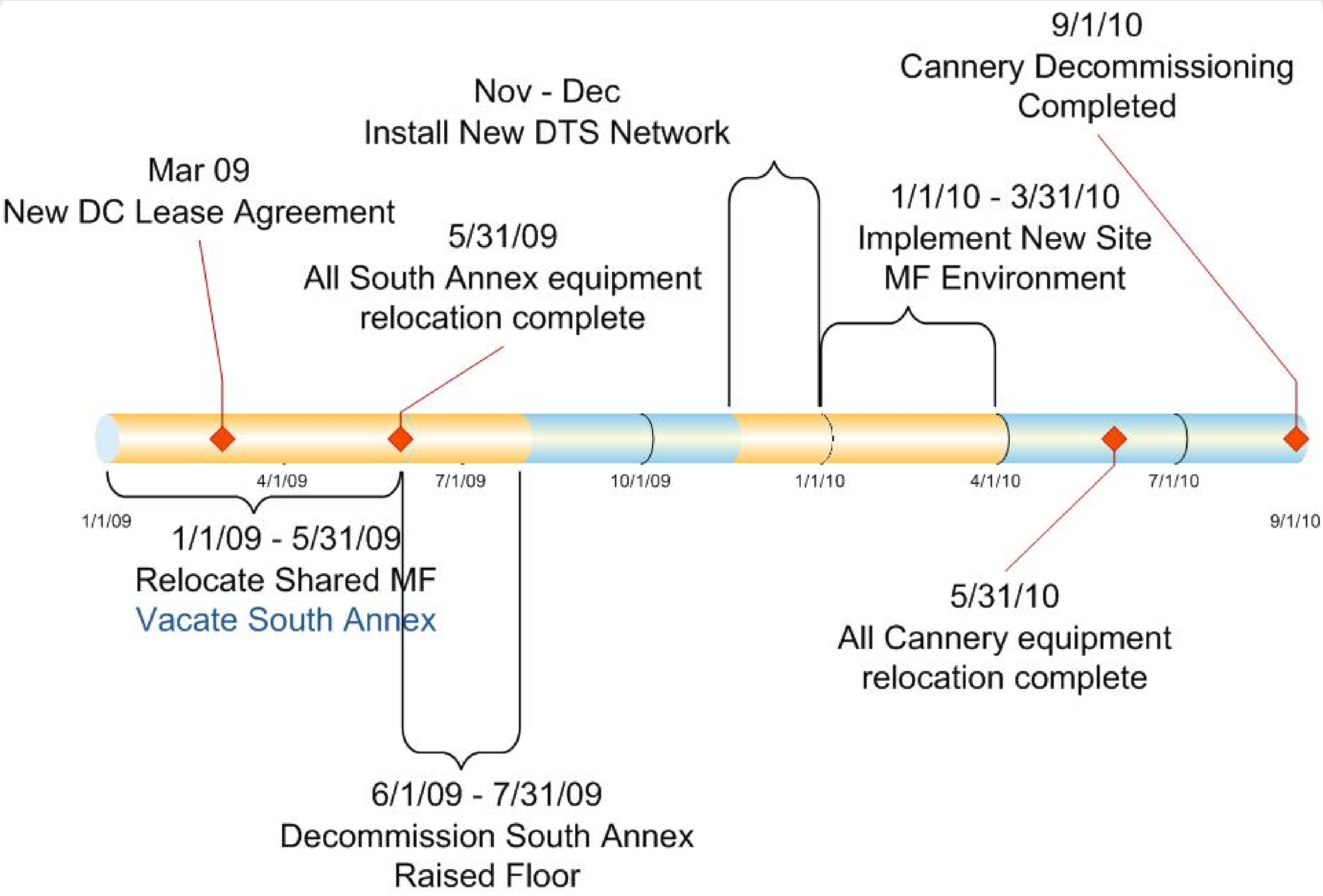
Major Considerations

Expiring Leases

Minimize Impact on rates

Minimize Customer Outages

Timeframe



Mar 09
New DC Lease Agreement

1/1/09 - 5/31/09
Relocate Shared MF
Vacate South Annex

5/31/09
All South Annex equipment
relocation complete

6/1/09 - 7/31/09
Decommission South Annex
Raised Floor

Nov - Dec
Install New DTS Network

1/1/10 - 3/31/10
Implement New Site
MF Environment

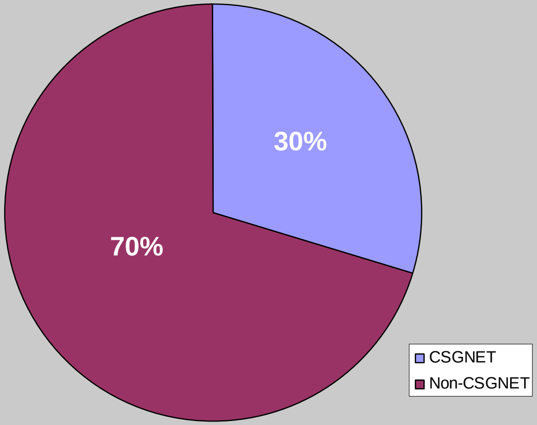
5/31/10
All Cannery equipment
relocation complete

9/1/10
Cannery Decommissioning
Completed

The Current Network

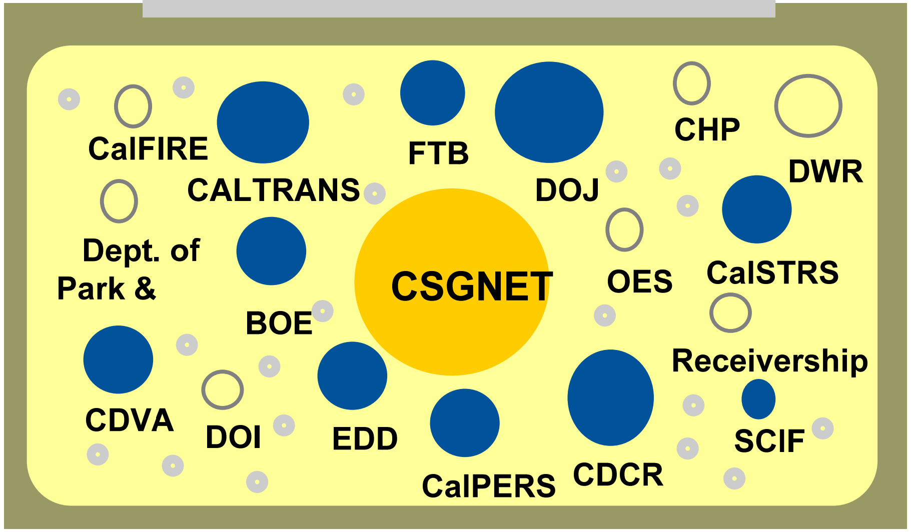
Big

- 6200 circuits
- 3500-4000 routers
- 50-100 separate networks
- 200-250 dedicated connections to external partners



30% of the circuits in the State are for CSGNET

Decentralized



New Network Strategy

- – An enterprise network with mandatory participation
- – MPLS Based
- – Move to a managed service model
- – Transform the role of DTS from network provider to service manager
- – Leverage both CALNET II providers
- – Transition all State agencies and departments within five years.

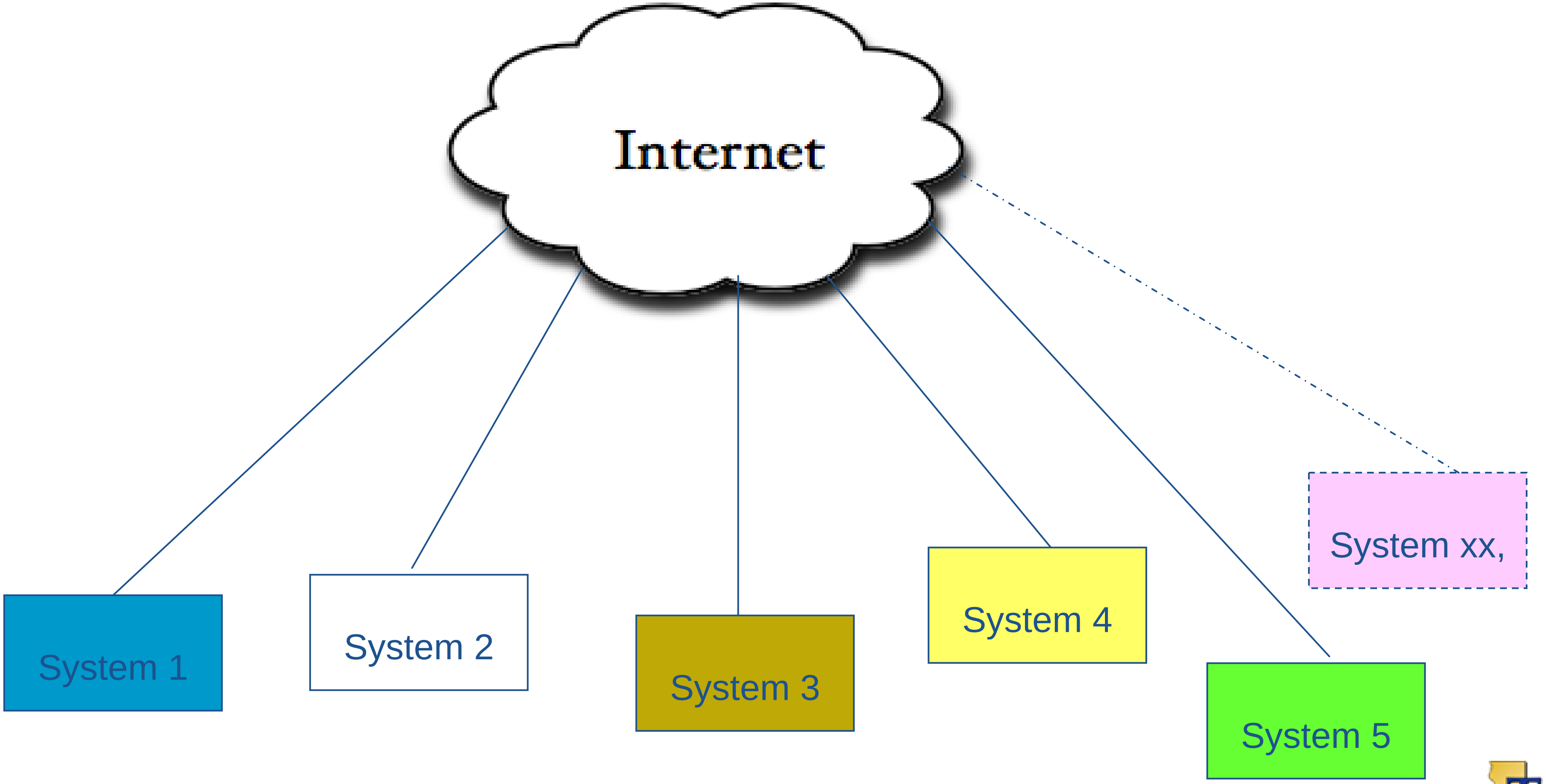
Implementation

- Migrate departments to managed networks
  - Shutdown CSGnet within 24 months
  - End-of-life migration
  - New or expanding departmental networks

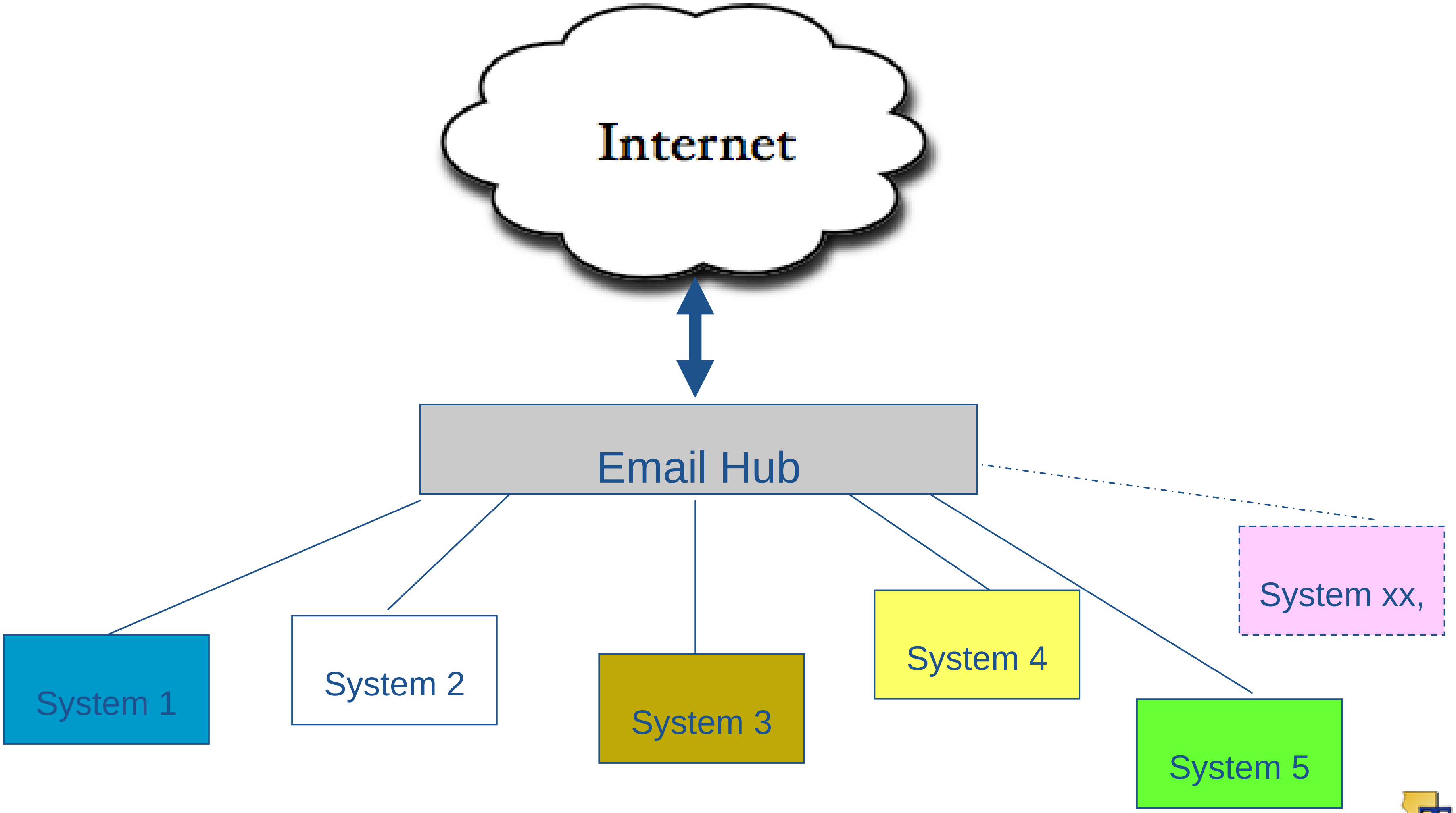
eMail Strategy

- Continue to enhance Statewide email
  - Exchange 2007
  - EHub
  - Statewide directory
  - eDiscovery
  - eFAX
  - Encryption
- Migrate departments on a volunteer basis

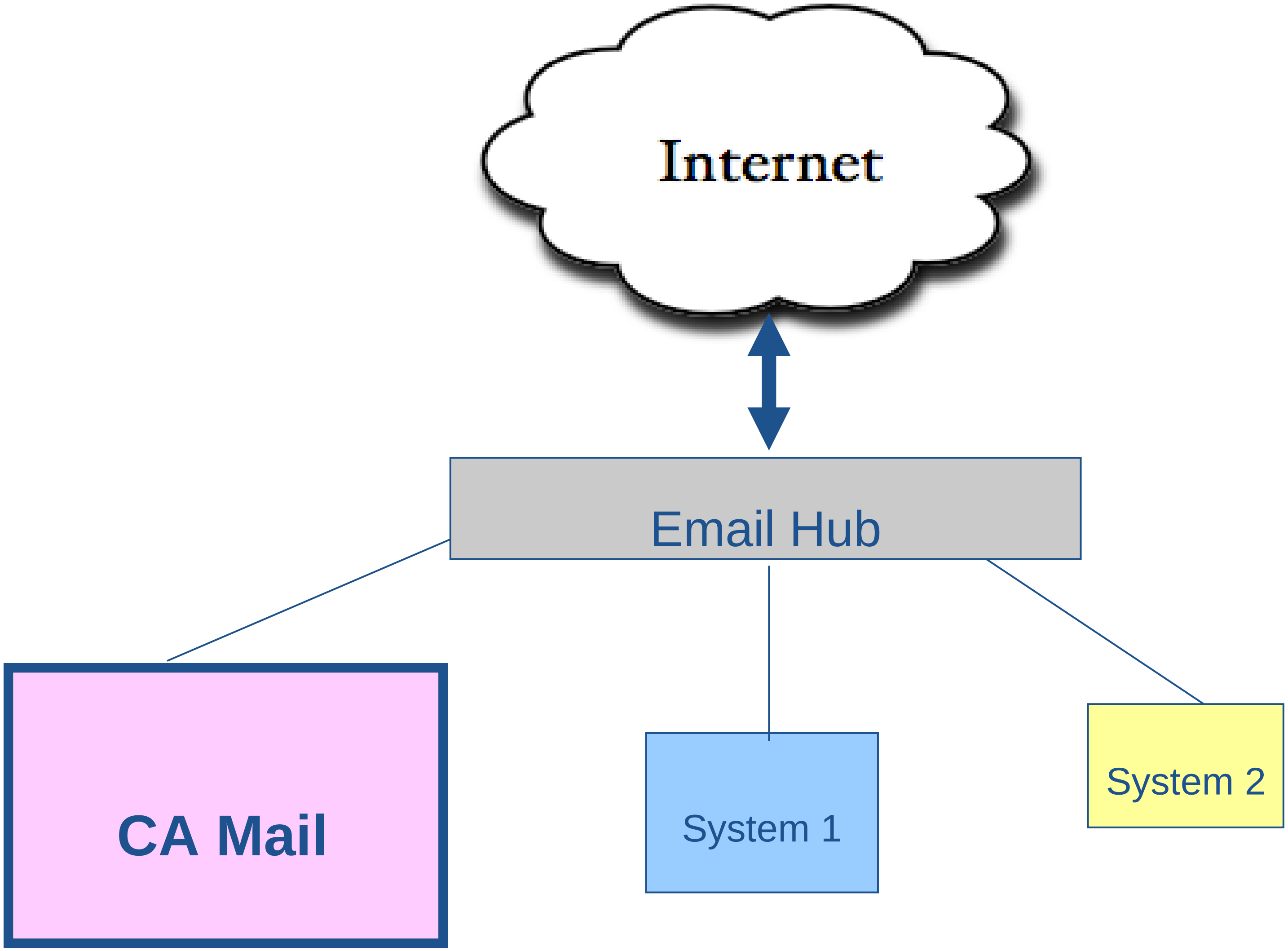
Current System, no E-Hub



Interim System-During E-Hub Migration

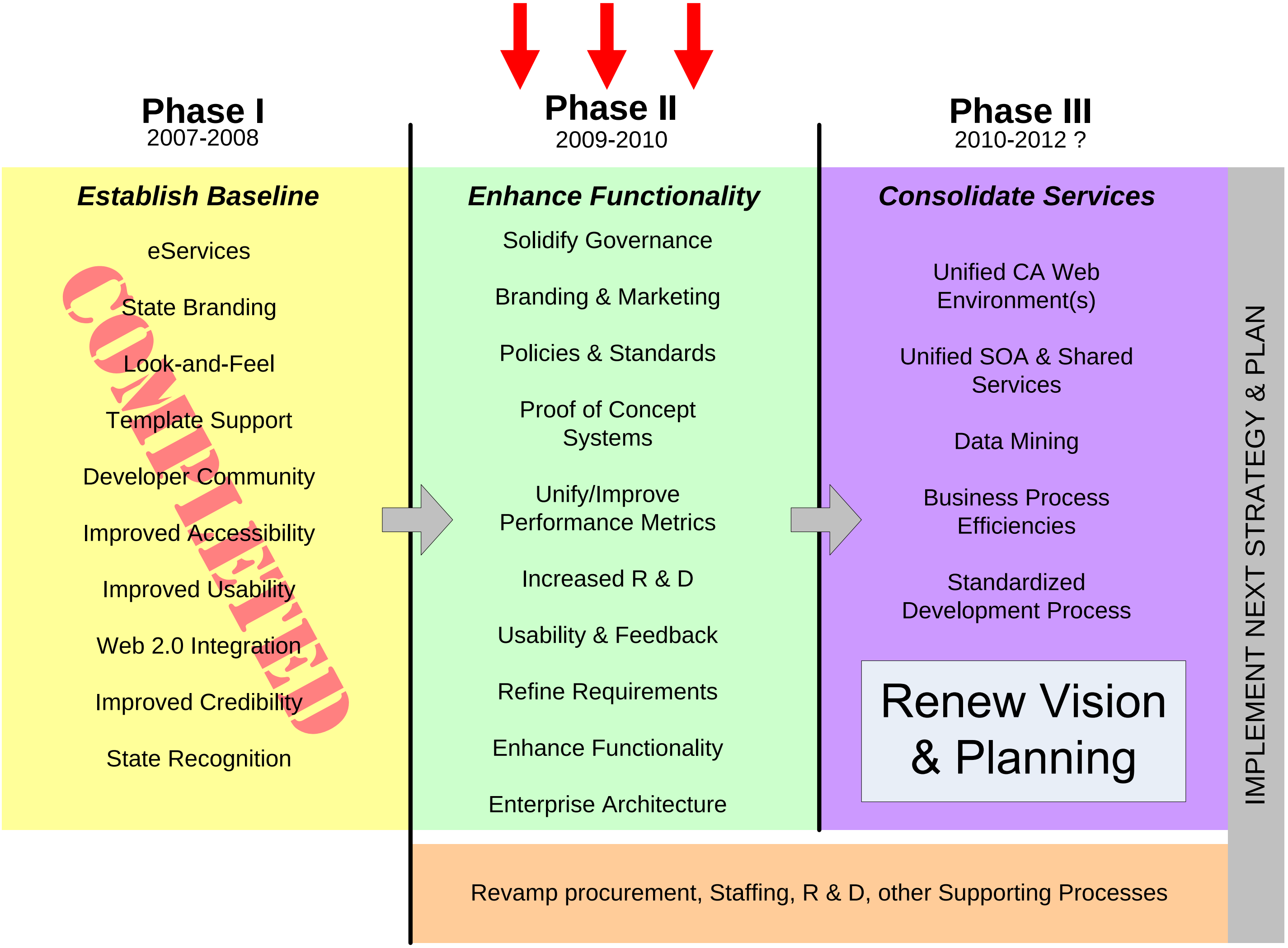


E-Hub, Full Implementation



What Are We Doing?

California State Portal Strategy



Phase I
2007-2008

Establish Baseline

eServices

State Branding

Look-and-Feel

Template Support

Developer Community

Improved Accessibility

Improved Usability

Web 2.0 Integration

Improved Credibility

State Recognition

COMPLETED

Phase II
2009-2010

Enhance Functionality

Solidify Governance

Branding & Marketing

Policies & Standards

Proof of Concept Systems

Unify/Improve Performance Metrics

Increased R & D

Usability & Feedback

Refine Requirements

Enhance Functionality

Enterprise Architecture

Phase III
2010-2012 ?

Consolidate Services

Unified CA Web Environment(s)

Unified SOA & Shared Services

Data Mining

Business Process Efficiencies

Standardized Development Process

Renew Vision & Planning

IMPLEMENT NEXT STRATEGY & PLAN

Revamp procurement, Staffing, R & D, other Supporting Processes

2009 Portal Plan

- Update/enhance existing portal services
- Add new functionality
- Incorporate innovative ideas
- Increase collaboration

DTS Strategic Projects

- **Identity Management**
- **Service Delivery Improvement**
- **Service Oriented Architecture**
- **Enterprise Storage**
- **Remote Management**
- **Service Continuity**
- **Enterprise Architecture**
- **Green**

Green

Green Purchasing Policy

Energy Audit and Monitoring (GC)

Green Team (promoting awareness)

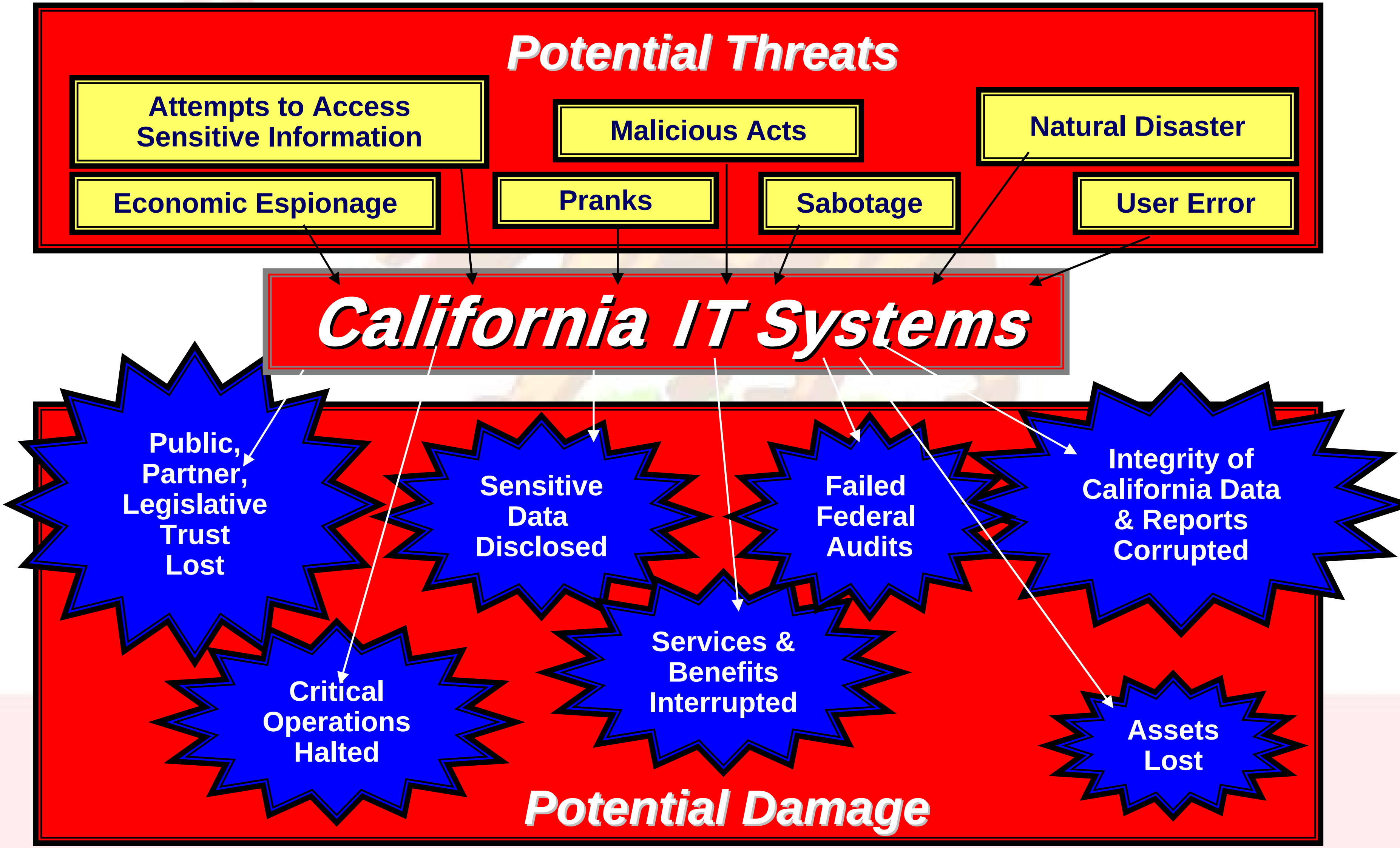
Governor’s LEED Silver requirement

Subject of IT Management Academy Class Project

The End

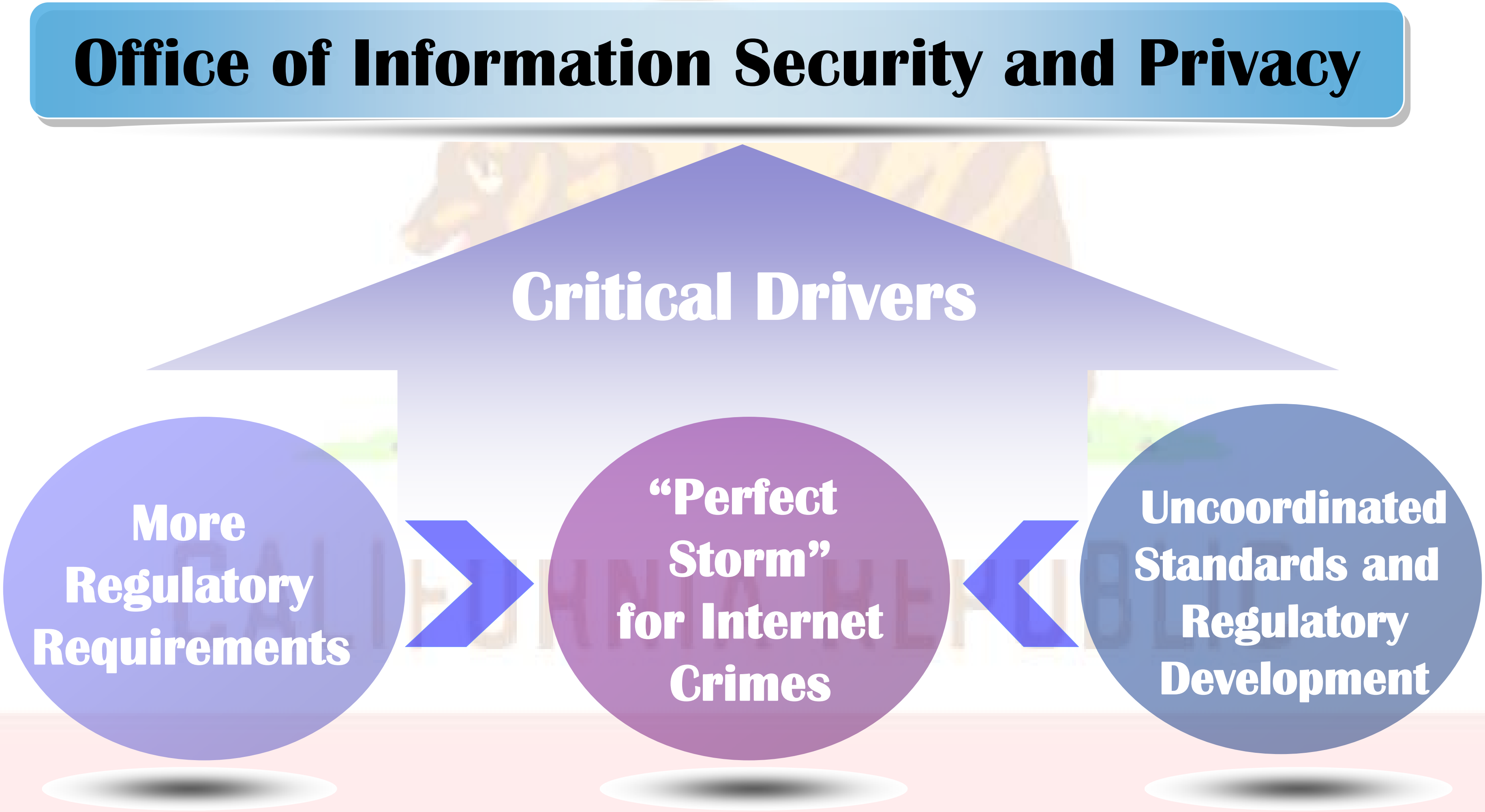
Mark Weatherford
California Office of Information Security and Privacy
February 23, 2009

Enterprise Security Risks



Potential Threats
Attempts to Access Sensitive Information
Malicious Acts
Natural Disaster
Economic Espionage
Pranks
Sabotage
User Error
California IT Systems
Public, Partner, Legislative Trust Lost
Sensitive Data Disclosed
Failed Federal Audits
Integrity of California Data & Reports Corrupted
Critical Operations Halted
Services & Benefits Interrupted
Assets Lost
Potential Damage

Security Program Drivers



Office of Information Security and Privacy

Critical Drivers

More Regulatory Requirements

"Perfect Storm" for Internet Crimes

Uncoordinated Standards and Regulatory Development

A Brief History of Regulatory Time

1970-1980

- ✓ **Privacy Act of 1974**
- ✓ **Foreign Corrupt Practice Act of 1977**

1980-1990

- ✓ **Computer Security Act of 1987**

1990-2000

- ✓ **EU Data Protection**
- ✓ **HIPAA**
- ✓ **FDA 21CFR Part 11**
- ✓ **C6-Canada**
- ✓ **GLBA**

2000-Present

- ✓ **COPPA**
- ✓ **USA Patriot Act 2001**
- ✓ **EC Data Privacy Directive**
- ✓ **CLERP 9**
- ✓ **CAN-SPAM Act**
- ✓ **FISMA**
- ✓ **Sarbanes Oxley (SOX)**
- ✓ **CIPA 2002**
- ✓ **Basel II**
- ✓ **NERC 1200 (2003)**
- ✓ **CISP**
- ✓ **Payment Card Industry (PCI)**
- ✓ **State Privacy Laws**

The “Perfect Storm” for Internet Crime

- 30-year old protocols with no security
- No taxes, therefore no tax evasion
- Value in everything online
- Anonymous access to vast resources
- Millions of clueless victims
- No national or political boundaries
- Laws and law enforcement are limited
- Virtually unlimited interconnectivity
- Criminal tools look and act like lawful tools
- Abundant opportunity for money laundering (PayPal, etc.)

Marcus Sachs

SANS Storm Center Diary – 11/11/07

Dangers of Uncoordinated Standards and Regulatory Development

Lack of consistency across state agencies with:

- Cross-boundary information sharing
- Cyber security threat identification and vulnerability management
- Public safety communications
- First responder credentialing
- Electronic health information exchange
- Enterprise Geographic Information System (GIS)

Think about it…

- For a traditional criminal to steal $1,000,000 there's not a lot of places they can go to commit the crime. The cyber criminal on the other hand only needs to steal $1.00 from a million people.
  - Who's going to notice or complain about $1.00?
  - What law enforcement organization is going to launch an investigation for a $1.00 crime?

> "Any organized crime group that isn't using these techniques should be sued for malpractice"
>
> ***Patrick Morrissey, US Secret Service, on the cyber crime epidemic***

Security Worries?

…7333 personal records stolen from home-worker

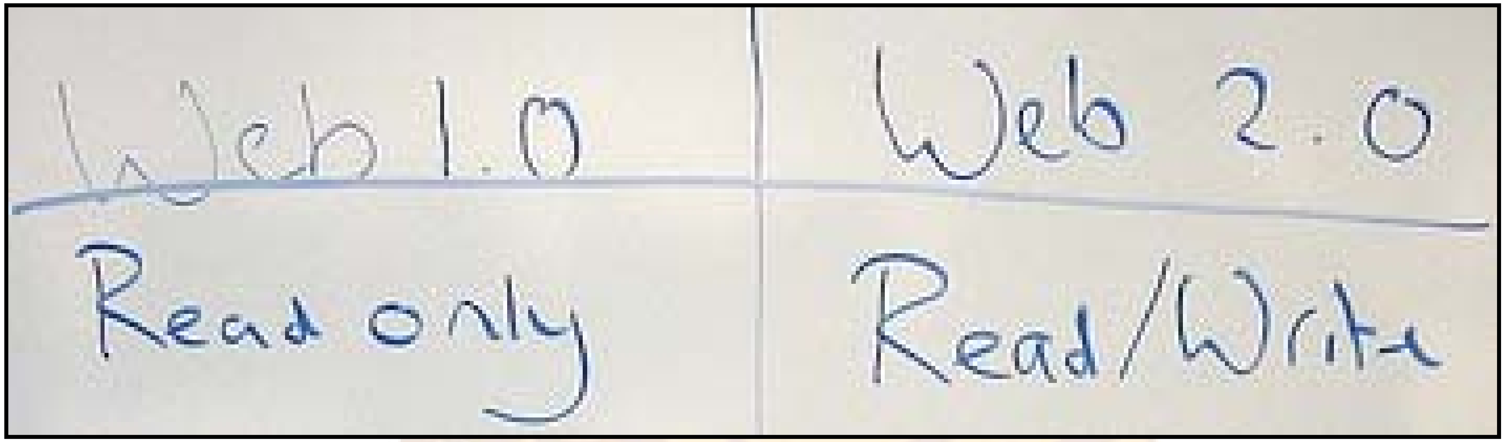
Economic Bust, Cybercrime Boom

State government computers part of international crime BOTNET

WEB 2.0 Vulnerabilities creating havoc for state governments

Computers in several states part of national cyber extortion case

Investigation of data theft reveals agency didn't have an employee policy for telecommuting…



Web 1.0	Web 2.0
Read only	Read/Write

Web 2.0 doesn’t define a technology, it defines a period in history! Read **AND** Write – be both an Author and Publisher

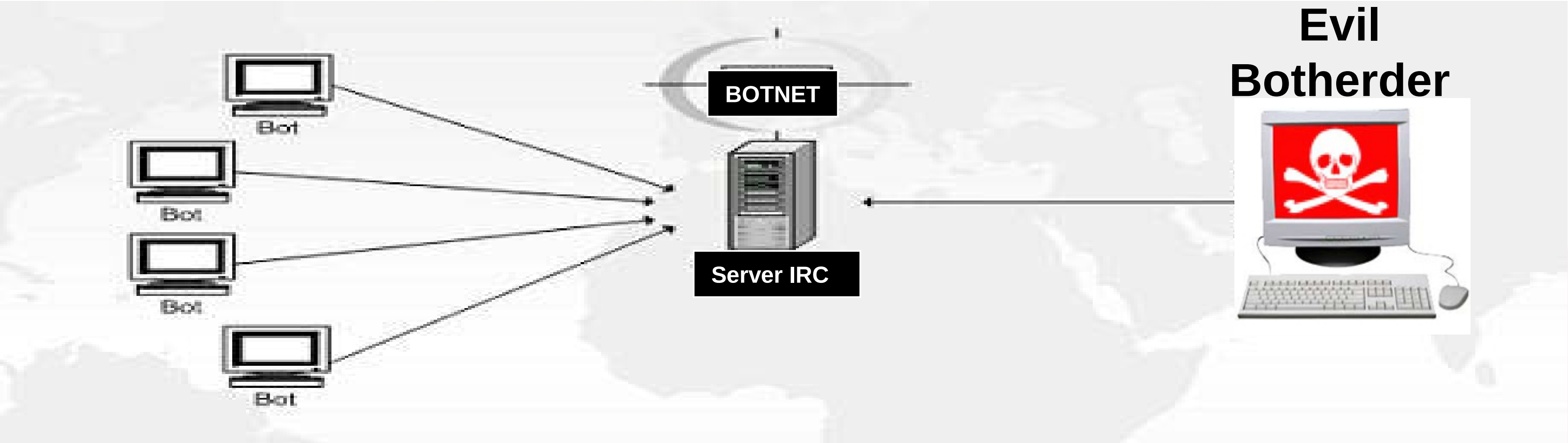
- Search (Google, Alternative Search Engines)
- Social Networks (MySpace, Facebook, OpenSocial)
- Online Media (YouTube, Last.fm)
- Content Aggregation / Syndication (Bloglines, Google Reader, Techmeme, Topix)
- Mashups (Google Maps, Flickr, YouTube)

Slide credit: Richard MacManus
Image credit: catspyjamasnz

Bots and Botnets: the next Killer App?

A Botnet is an infrastructure of compromised Bot computers (zombies) infected with remote control software used by criminals to commit crime and make money by:

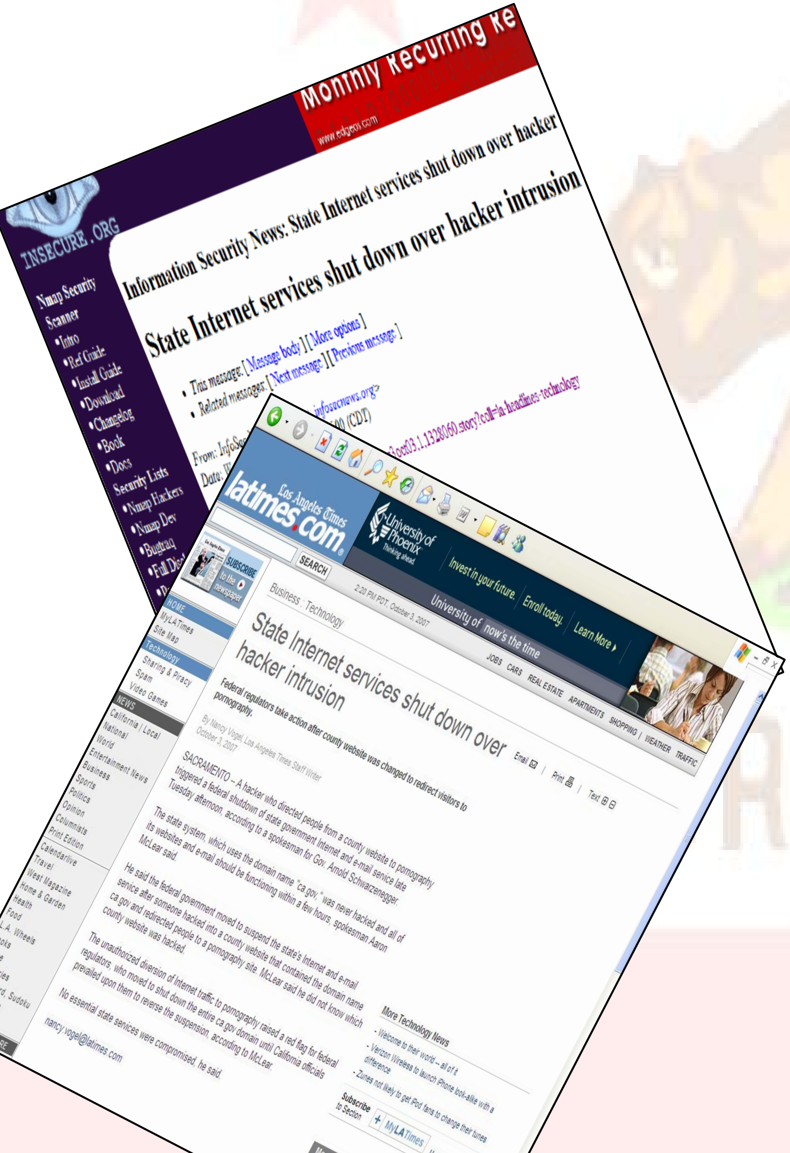
- Spamming
- DDoS
- Phishing Attacks
- Worms
- Sniffing Passwords
- Keystroke Logging
- Identity theft
- Hosting Illegal Software



TeleWork Security Issues

- Secure Remote Access/Virtual Privacy Network (VPN)
- Full-disk encryption on mobile devices
- Unauthorized Access to State Networks
- Configuration Management
- Unauthorized Data Access
- Remote Access Monitoring
- Network Access Control (NAC) for system updates/patches
- Two-factor authentication including tokens

ca.gov Incident



Monthly Recurring Re

www.edgeos.com

INSECURE.ORG

Nmap Security Scanner
- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists
- Nmap Hackers
- Nmap Dev
- Bugtraq
- Full Disc

Information Security News: State Internet services shut down over hacker

State Internet services shut down over hacker intrusion

- This message: [Message body] [More options]
- Related messages: [Next message] [Previous message]

From: InfoSe… infosecnews.org>
Date: W… 00 (CDT)

…3oct03,1,1328060.story?coll=la-headlines-technology

latimes.com Los Angeles Times

SEARCH

SUBSCRIBE to the newspaper

University of Phoenix Thinking ahead. Invest in your future. Enroll today. Learn More ▸ University of now's the time

JOBS CARS REAL ESTATE APARTMENTS SHOPPING | WEATHER TRAFFIC

HOME
MyLATimes
Site Map

Technology
Sharing & Piracy
Spam
Video Games

NEWS
California | Local
National
World
Entertainment News
Business
Sports
Politics
Opinion
Columnists
Print Edition
Calendarlive
Travel
West Magazine
Home & Garden
Health
Food
L.A. Wheels

Business : Technology

2:20 PM PDT, October 3, 2007

State Internet services shut down over hacker intrusion

Email ✉ | Print 🖶 | Text ⊕ ⊖

Federal regulators take action after county website was changed to redirect visitors to pornography.

By Nancy Vogel, Los Angeles Times Staff Writer
October 3, 2007

SACRAMENTO -- A hacker who directed people from a county website to pornography triggered a federal shutdown of state government Internet and e-mail service late Tuesday afternoon, according to a spokesman for Gov. Arnold Schwarzenegger.

The state system, which uses the domain name "ca.gov," was never hacked and all of its websites and e-mail should be functioning within a few hours, spokesman Aaron McLear said.

He said the federal government moved to suspend the state's Internet and e-mail service after someone hacked into a county website that contained the domain name ca.gov and redirected people to a pornography site. McLear said he did not know which county website was hacked.

The unauthorized diversion of Internet traffic to pornography raised a red flag for federal regulators, who moved to shut down the entire ca.gov domain until California officials prevailed upon them to reverse the suspension, according to McLear.

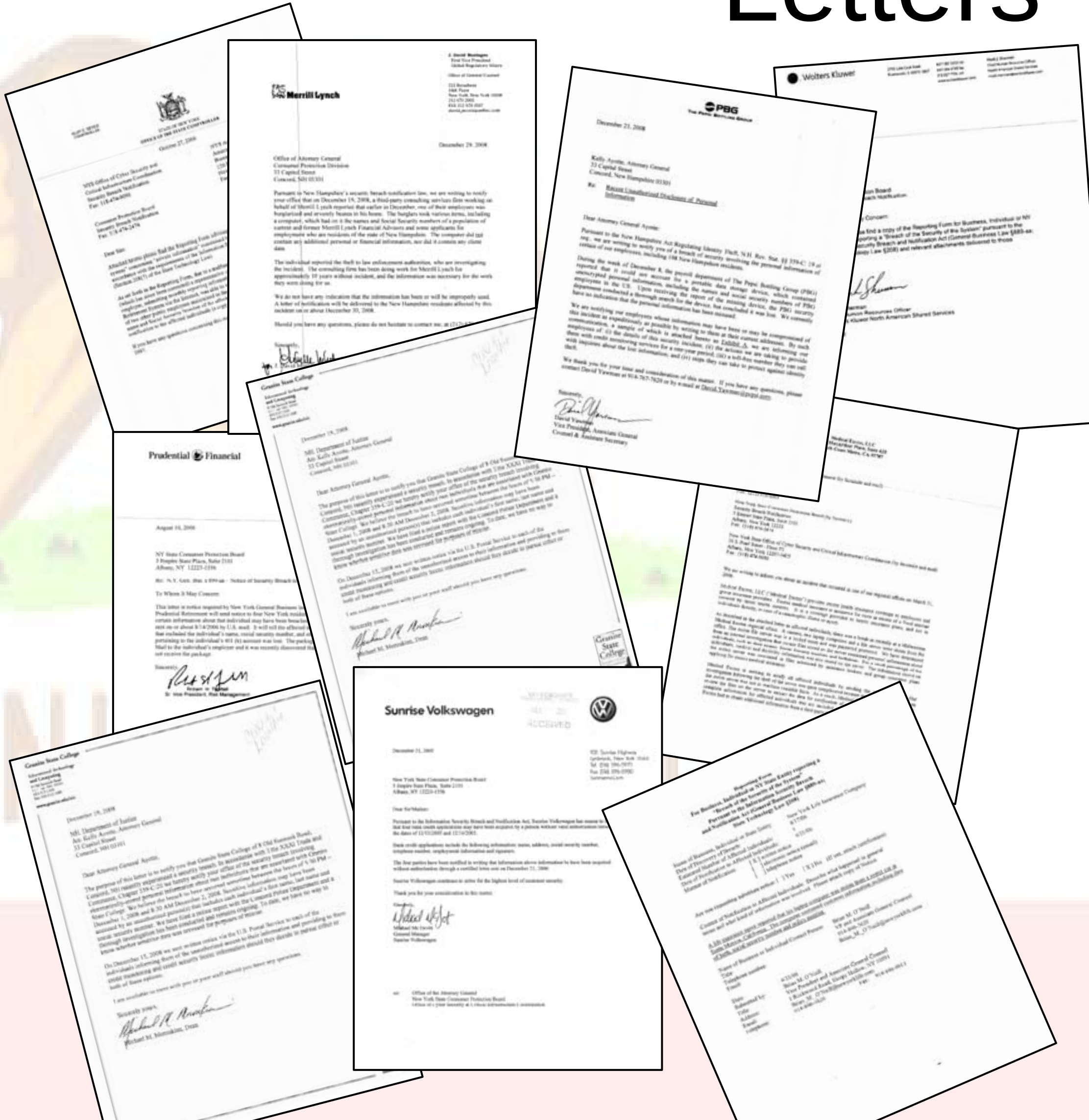
No essential state services were compromised, he said.

nancy.vogel@latimes.com

More Technology News
- Welcome to their world -- all of it
- Verizon Wireless to launch iPhone look-alike with a difference
- Zunes not likely to get iPod fans to change their tunes

Subscribe to Section + MyLATimes

Breach Notification Letters



Merrill Lynch

PBG The Pepsi Bottling Group

Wolters Kluwer

Prudential Financial

Granite State College

Sunrise Volkswagen

What’s Broken and How Do We Fix It?

1. Application and Web Development Security
2. Inconsistent O/S Configurations
3. System Patching
4. Perimeter Protection and User Awareness

After all these years, this stuff is still broken?

App Development is STILL broken!

- As many as 80 new software vulnerabilities are discovered every week (ControlScan©)
- Over 70% of web applications on-line today have exploitable security vulnerabilities (Cenzic©)
- Higher Ed and technical schools still do not (adequately) teach secure application coding
- Insecure code is no longer acceptable
- Developers and application vendors must step up and be accountable

Web Application Security

For example:

- 17,000,000 programmers
- 102,000,000,000 LOC/year
- 162,000,000 websites on-line
- 9 out of 10 websites with at least one vulnerability
- Researchers estimate one security defect per 10,000 LOC
- If only 1% of vulnerabilities are exploitable that equals 102,000 zero days/year

Jeremiah Grossman

CSO online – July 2, 2008

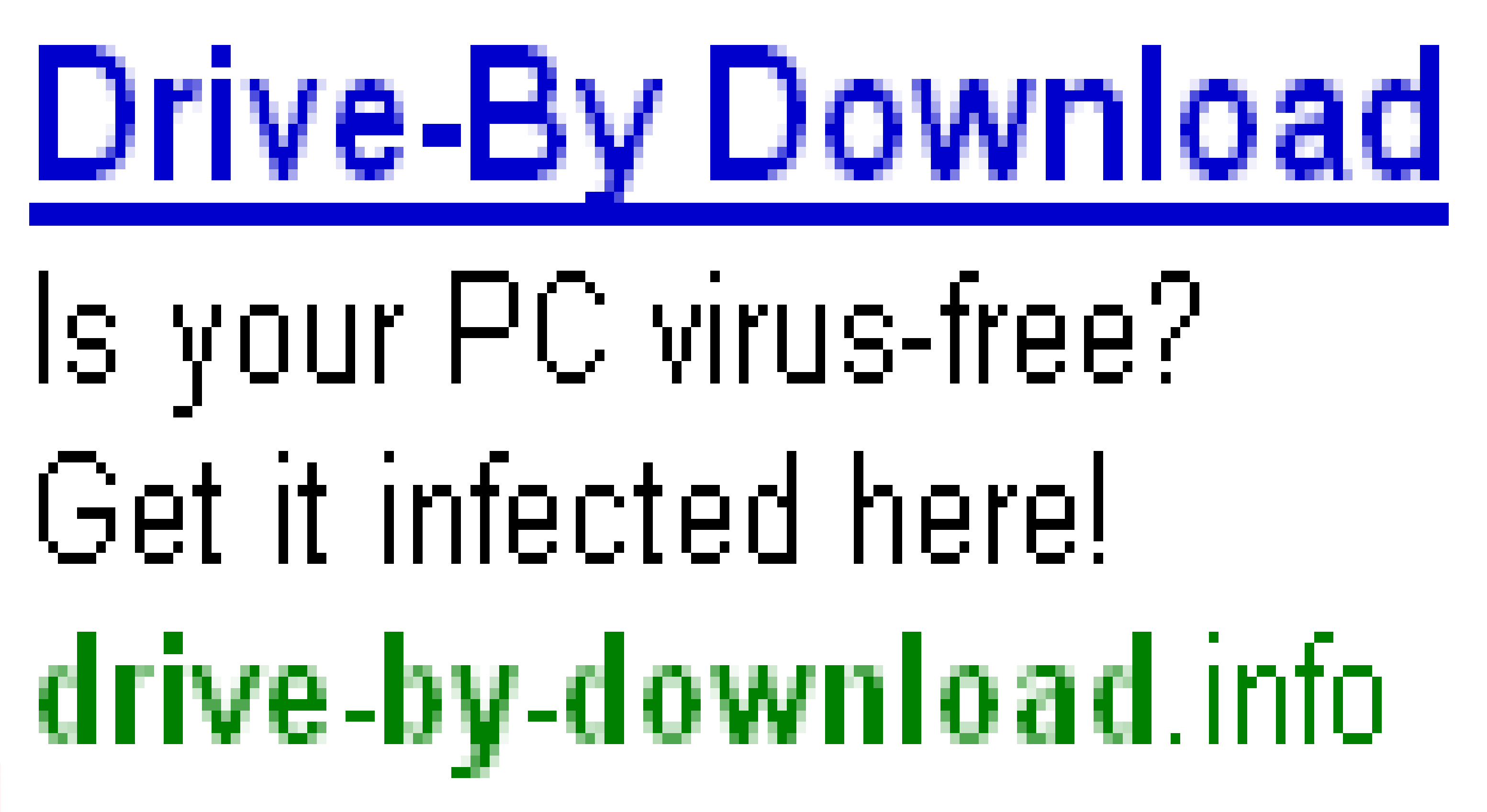
O/S Configurations Management is STILL Broken!

- This is a policy issue
- Federal Desktop Core Configuration (FDCC) Application vendors now have to certify that their applications:
    1. Do not require regular users to have administrative privileges
    2. Run on the standard secure configurations (674 individual settings/services)
    3. Do not change the secure configurations

Patching Is Still Broken!

- Think about it. Every month we get “updates” to fix something in the vendor’s code???
- Vulnerabilities are exploited before patches are installed
  - 0Day exploits
- Why?
  - Still a post-facto exercise
  - Applications require non-standard configurations
  - Patches must be tested on all applications in your environment to avoid breaking applications

User Awareness (and Perimeter Security) Is Still Broken!



Drive-By Download

Is your PC virus-free?

Get it infected here!

drive-by-download.info

Challenging

CIO

BUSINESS TEC LOG EA RS P

3 SECRETS OF PROJECT MANAGEMENT SUCCESS

The people, the pro the tools

TO A
UT RC DE
s n st ab gett to y
Page 66

MO LIZE YOUR
PRISE APPS
How to overcome the obstacles
Page 25

THE ~~GLOBAL~~ Confusing STATE OF INFORMATION SECURITY

ere's good news and there's bad news...

83% of you align security policies with business goals, **but...** **57%** of you don't monitor compliance with security policies.

75% of you are confident in partners' security, **but... 72%** of you don't examine how third parties handle personal data.

83% of you believe your security practices are effective, **but...** **44%** of you don't know how security incidents happened.

What It All Means, What to Do Next

BY KIM S. NASH

Exclusive research begins on Page 45

OCTOBER 15, 2008 | $9.00 | CIO.COM

What is California doing to protect sensitive citizen and employee information and government assets while making it harder for criminals, attackers and naive users?

Office of Information Security and Privacy Protection

Senate Bill 90 (2007) formally established the Office of Information Security and Privacy in January 2008. The legislation provides the following authority:

- **Information Security & Privacy**
  - Develop policies, standards and procedures
  - Provide assistance, advice and training
  - Conduct compliance monitoring
  - Direct audits and assessments as required
- **Consumer Privacy Program**
  - Provide information and assistance
  - Provide education for consumers, business, and law enforcement
  - Develop recommended practices for organizations

OISPP ***Priorities***

1. Enterprise Security Strategic Plan
2. Enterprise Information Security Policy Gap Analysis
3. Enterprise Threat and Vulnerability Management Program (TVMP)
4. Streamline procurement for security products and services
5. Automated Incident Response Reporting process
6. Cyber security training and user awareness
7. Security oversight of application development projects

Enterprise Security Strategic Plan

- **Goal**
  - develop a strategic plan to guide OISPP’s activities and initiatives over the next 5 years
- **Key Tasks**
  - Review current activities and focus of OISPP
  - Streamline the focus of OISPP to a small number of areas where the greatest impact within state agencies may be achieved in the areas of security and privacy
- **Benefits to agencies**
  - Increased visibility and transparency of OISPP
  - Streamlined processes for improved response to agencies
  - Improved security and privacy through simplified assessment of agency risks
  - Consistent expectation of services

Policy Gap Analysis

- **Goal**
  - Establish comprehensive, standards-based policies to address security and privacy threat landscape, risks, and vulnerabilities
- **Key Tasks**
  - Identify gaps in existing information security policies
  - Develop and revise policies to align with current environment
  - Draft standards and procedures to support security policies
- **Benefits to agencies**
  - Improvement in the consistency and coverage of policies by addressing security areas and risks that have been gaps or are emerging (e.g., mobile computing, data privacy)
  - Reduction in overlap and redundancy
  - Simplification of policies to increase readability and usability
  - Establish information security baseline

Threat and Vulnerability Management Program (TVMP) Services

The TVMP will evaluate threats and vulnerabilities to California state agency systems and provide consultative support for mitigation strategies. The TVMP service will *eventually* consist of the following offerings:

1. Policy and Planning Consulting services
2. External Vulnerability Assessment services
3. Internal Vulnerability Assessment services
4. Vulnerability Remediation services
5. Penetration Testing services
6. Social Engineering Assessment services
7. Web Application Assessment services
8. Firewall/ACL Assessment services
9. Wireless Security Assessment services

Security Products and Services Procurement

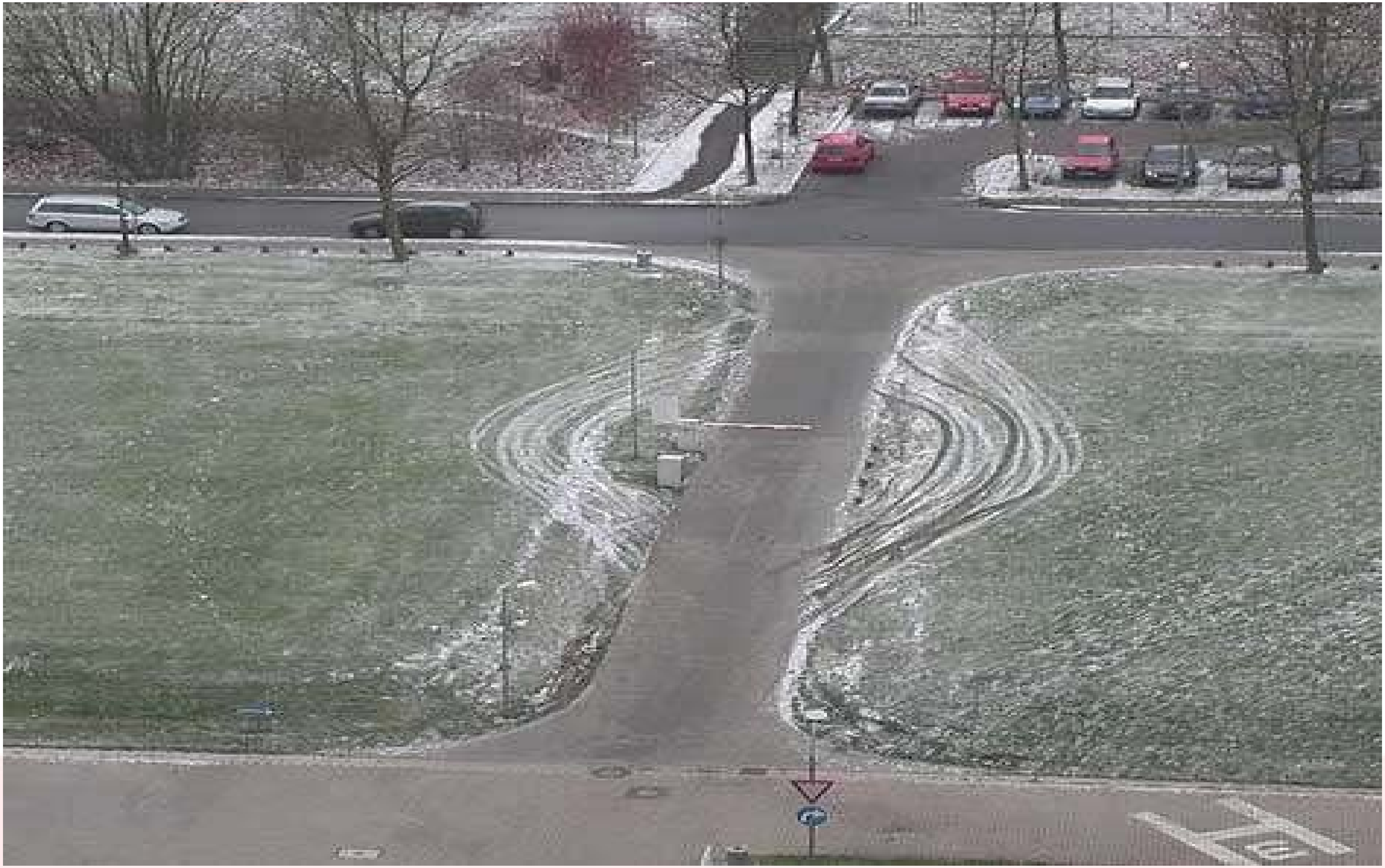
The vast number of vendors can be overwhelming for agencies needing to procure security products and services. Goal:

- Use existing leveraged procurement vehicles such as the California Multiple Award Schedule (CMAS), SLP, CalNet/CalNet II and Master Service Agreements (MSA).
- Identify the desired security products and services and the existing procurement vehicles.
- Identify the vendors that have existing security products and services available.

The To-Do List

- SDCC (State Desktop Core Configuration)
- Enterprise information security risk assessment(s)
- Data Loss Prevention (DLP)
- Critical Infrastructure (SCADA/Control system)
- Payment Card Industry (PCI)
- California Information Sharing and Analysis Center (CA-ISAC)
- Enterprise encryption (DAR and DIT)
- Federated Identity Management across the enterprise

The Security Challenge…



mark.weatherford@oispp.ca.gov